IN THE CLAIMS:

1. (Original) A method for variably generating cryptographic securities, for communications, in a host device, comprising the steps of:

for cryptographically securing a communication for a first purpose, using a first signature;

for cryptographically securing a communication for a second purpose, using a second signature; and

using a cryptographic algorithm of a first type to generate said first signature and using a cryptographic algorithm of a second type to generate said second signature.

2. (Original) A method as claimed in claim 1 comprising:

storing a program in a read only memory of a postal security device for implementing the respective cryptographic algorithms for generating said first and second signatures; and

implementing at least one of the cryptographic algorithms for generating at least one of the first and second signatures in a hardware unit outside of and in communication with said postal security device.

3. (Original) A method as claimed in claim 1 comprising implementing the respective cryptographic algorithms to generate said first and second signatures in respective, separate logic modules, and generating the first and second signatures in the respective logic modules under control of a program.

4. (Original) A method as claimed in claim 1 comprising:

storing a plurality of signing algorithms and hash algorithms in a read only memory of a postal security device; and

in a logic module having access to said read only memory, implementing at least one of said signing algorithms and hash algorithms as a cryptographic algorithm for generating one of said first and second signatures, dependent on whether the communication is for said first purpose or said second purpose.

5. (Original) A method as claimed in claim 4 comprising implementing said at least one of said signing algorithms and hash algorithms exclusively in said logic module alone.

6. (Original) A method as claimed in claim 4 comprising storing an implementation program in said postal security device and implementing said at least one of said signing algorithms and hash algorithms in said logic module using said implementation program.

7. (Original) A method as claimed in claim 4 comprising storing an implementation program in said host device and implementing said at least one of said signing algorithms and hash algorithms in said logic module using said implementation program.

Claims 8-19 are cancelled.

8-19. (Cancelled)